REMARKS

Claims 1-16 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 112, First Paragraph, Rejection:

The Examiner rejected claims 1, 6, 11 and 16 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Applicants respectfully traverse this rejection for at least the following reasons.

In the current office action of August 6, 2008, the Examiner maintains his previous rejection of claims 1, 6, 11, and 16 under 35 U.S.C. 112, asserting again that Applicants' specification does not define "quiesce time." Applicants draw the Examiner's attention to the following portions of the specification. The emphasis is added:

> [0006] In distributed shared storage environments where multiple clients may need simultaneous access to the same data, datasets may be fixed into specific versions to ensure data integrity across client sessions. These dataset versions may be referred to as file images. Certain tasks, like backing up one or more files, checking and correcting data consistency across mirrored database files, or virus removal may **require a single application or process to have exclusive access to one or more file images**. Typically, **general access to the datasets involved must be *quiesced*** and all data caches must be flushed. Freezing the I/O to a specific file or dataset image in a shared storage environment may require the MDS to individually cancel all current access tokens by transmitting recall or revocation messages to every client that has been issued access tokens for the image. Revoking access tokens individually may be burdensome with numerous outstanding tokens.
>
> [0007] When quiescing data I/O in a distributed shared storage environment, a metadata server (MDS) may **set the expiration time on issued access tokens to be no later than a scheduled *quiesce time***. The MDS may maintain one or more scheduled **quiesce times**. **Client applications requiring *exclusive access to files or datasets* may contact a MDS and request a quiesce time.** The MDS may use the scheduled

quiesce to determine whether to set the expiration time in access tokens using a default expiration time, or to use an expiration time based upon the next scheduled quiesce time. Storage devices may recognize and enforce expiration times in tokens. Storage devices may deny data I/O requests from clients presenting expired access tokens. Trusted applications may schedule **quiesce times** to perform systems tasks such as file backup and recovery, mirror synchronization, database repair and compacting, among others. The MDS may provide an interface to allow such clients to schedule a **quiesce time**. When quiescing data I/O, the MDS may use expiration times in access tokens to avoid sending an individual revocation message to each client for each access token held by that client, and may assume that all relevant access tokens have expired at or prior to the **quiesce time**. [emphasis added]

[0015] Figure 1 illustrates a computer network, according to certain embodiments, in which one or more devices may be configured to implement a distributed shared storage environment that may utilize the expiration of access tokens to **quiesce data I/O to file images for frozen image generation, backups, mirror synchronization and other tasks requiring exclusive file image access**. The **quiescing of data I/O may be scheduled in advance**, in some embodiments. **Quiesce times** may be scheduled to occur periodically, or may be scheduled individually or otherwise, according to various embodiments. In one embodiment, at least one computing device on a network 100 may be a client device, such as Client 110 or Client 120 with installed software that may be configured to communicate with other devices, acquire access tokens, and exchange data with data storage devices. In one embodiment, at least one computing device on Network 100 may be a server device, such as Metadata Server 130 with installed software that may be configured to **maintain a scheduled quiesce time and to provide access tokens with expiration times**.

[0034] Figure 4B, illustrates, according to one embodiment a method for a client to **schedule a quiesce time**. A client, such as Client 100, may be a trusted client responsible **for tasks that require exclusive access to certain files or dataset images**. For example, a backup program needs to be sure that a file isn't being changed at the same time it is being backed up. In one embodiment, a client may contact a metadata server, such as Metadata Server 130 and **request the scheduling of a quiesce time**, as illustrated in block 480. **In response to such request a metadata server may verify that the client is allowed to schedule a quiesce time and if so, the metadata server may set a next scheduled quiesce time**, such as Next Scheduled Quiesce Time 215 illustrated in Figure 2. After scheduling the **quiesce time**, the client may wait, possibly performing other tasks, until the scheduled **quiesce time**.

These excerpts in the specification clearly delineate the notion of quiesce time, and thus the phraseology found in Applicants' independent claims is well-supported in the specification. As long as the description "allows persons of ordinary skill in the art to recognize that [the inventors] invented what is claimed" then the description requirement is satisfied. *In re Gosteli*, 10 USPQ2d 1614, 1618 (Fed. Cir. 1989). "The subject matter of the claim **need not be described literally** in order for the disclosure to satisfy the description requirement." *M.P.E.P. 2163.02*. As shown above, when Applicants' specification is considered as a whole, one skilled in the art would easily recognize the claimed invention. The Examiner's application of the written description requirement in the Final Action is "yet another instance of the sort of 'hypertechnical application' of the written description requirement of §112" that has been repeatedly criticized by the court. *In re Driscoll*, 195 USPQ 434, 438 (C.C.P.A. 1977); *In re Johnson*, 558 F.2d 1008, 194 USPQ 187 (CCPA 1977); *Engineering Development Laboratories v. Radio Corp. of America*, 68 USPQ 238, 241-42 (2d Cir. 1946). Withdrawal of this rejection is respectfully requested.

The Examiner also incorrectly asserts that "the word 'quiesce' is very rarely used. In fact, the word "quiesce" occurs often within the realm of computation, and is used in many modern patents in computer technology. In particular, the term "quiesce" is frequently used with a well understood meaning in the art of storage technology that is consistent with how the term is used in Applicants' claims. Applicants note that the Examiner cites a patent of Hart, 6,983,295, which uses the word "quiesce." Applicants' usage of the word "quiesce" is consonant with conventions readily understood and accepted by those skilled in the relevant arts of storage technology.

In the Response to Arguments of the current Office Action of August 6, 2008, the Examiner has made no attempt to address the substance of the Applicants' remarks concerning the rejection under 35 U.S.C. 112, writing dismissively "Applicant argument is not persuasive to consider as 'need not be described literally (sic).'" The Examiner's statements do not show that one skilled in the art would not recognize that the inventors had possession of the invention at the time the application was filed. **The Examiner has**

the burden of presenting evidence or reasons why persons skilled in the art would not recognize in the disclosure a description of the claimed invention. *Ex parte Sorenson*, 3 USPQ2d 1462, 1463 (Bd. Pat. App. & Inter. 1987). The Examiner has not met his burden for presenting evidence or reasons why persons skilled in the art would not recognize in the disclosure a description of the claimed invention. The Board has held that "**a bare assertion by the Examiner**" is insufficient for an assertion that the description requirement is not met. *Sorenson*, 3 USPQ2d at 1463 (Bd. Pat. App. & Inter. 1987). The Examiner has the burden to present evidence or reasons, not just bare assertions, why persons skilled in the art would not recognize support for the claimed invention. *In re Wertheim*, 191 USPQ 90 (CCPA 1976). Thus, the Examiner has not stated a *prima facie* rejection. As repeatedly stated by the Board of Patent Appeals & Interferences and by the Court of Appeals for the Federal Circuit, it is well settled that the claimed invention does not have to be described in *ipsis verbis* in order to satisfy the description requirement of §112. *Jacobs v. Lawson*, 214 USPQ 907, 910 (B.P.A.I. 1982). "The subject matter of the claim need not be described literally in order for the disclosure to satisfy the description requirement." *M.P.E.P. 2163.02*.

Section 101 Rejection:

The Office Action rejected claims 6-16 under 35 U.S.C. § 101 as allegedly not being directed to statutory subject matter. Applicants respectfully traverse this rejection for at least the following reasons.

In the Response to Arguments, the Examiner asserts, without elaboration, that the Applicants "did not properly amend claims to overcome the rejection." The Examiner may have overlooked the amendments made to claims 6 and 11. Claim 6 was amended to recite a processor and a memory storing program instructions executable by the processor to implement a metadata server, and claim 11 was amended to recite a computer-readable, storage medium storing program instructions that are–computer-executable. As noted in MPEP 2106.01, "[w]hen functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally

interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized." *See, e.g.*, *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035.

In regard to claim 16, Applicant reiterate their previous assertion that according to the section of the MPEP on Patentable Subject Matter Eligibility, MPEP 2106.II.C, "Where means plus function language is used to define the characteristics of a machine or manufacture invention, such language must be interpreted to read on only the structures or materials disclosed in the specification and "equivalents thereof" that correspond to the recited function. Two *en banc* decisions of the Federal Circuit have made clear that the USPTO is to interpret means plus function language according to 35 U.S.C. § 112, sixth paragraph. *In re Donaldson*, 16 F.3d 1189, 1193, 29 USPQ2d 1845, 1848 (Fed. Cir. 1994) (en banc); *In re Alappat*, 33 F.3d 1526, 1540, 31 USPQ2d 1545, 1554 (Fed. Cir. 1994) (en banc)." The structures and materials disclosed in Applicants' specification clearly include computer hardware [0015, 0021, 0032, 0036, 0037]. Therefore, the rejection of claim 16 is improper.

Withdrawal of this rejection is respectfully requested.

Section 103(a) Rejections:

The Office Action rejected claims 1, 3-6, 8-11 and 13-15 under 35 U.S.C. § 103(a) as being unpatentable over Schmeidler et al. (U.S. Patent 6,374,402) (hereinafter "Schmeidler") in view of Hart (U.S. Patent 6,983,295) and Ribot (U.S. Publication 2003/0187993), and claims 2, 7, 12 and 16 as being unpatentable over Schmeidler in view of Hart, McBrearty et al. (U.S. Publication 2004/0015585) (hereinafter "McBrearty") and in view of Ribot. Applicants respectfully traverse these rejections for at least the following reasons.

In regard to claim 1, contrary to the Examiner's assertion, the cited art does not teach or suggest in response to a metadata server receiving a data access request from a

client, the metadata server determining a maximum expiration time indicated by a next scheduled quiesce time, as recited in claim 1. The Examiner refers to Schmeidler, FIG.8, and to column 22, lines 48-54 and lines 59-66, as teaching this aspect of Applicants' claim. However, the cited portion of Schmeidler actually refers to a token authorizing a client to access a purchased title from a network file server (a Random Access File Transport (RAFT) server). The token, illustrated in FIG. 8 as RAFT token 800, contains a start-time element 806 and an end-time element 808, which define the **time *interval*** during which the client may access a particular resource, namely the title the client has purchased. This has no bearing whatsoever on a metadata server determining a **maximum expiration time *indicated by a next scheduled quiesce time***. The time interval of Schmeidler's token specifies a particular **time *period*** during which the client may access a purchased resource. It does not indicate a **maximum expiration time *indicated by a next scheduled quiesce time***, which is a time at which exclusive access to certain data is required by a task. Moreover, the token of Schmeidler is provided not by the network file server (RAFT server), but by the conditional access server (CAS). Thus, Schmeidler clearly does not describe in response to a metadata server receiving a data access request from a client, the metadata server determining a maximum expiration time indicated by a next scheduled quiesce time. Nor do any of the other cited references teach this aspect of Applicants' claim, whether considered alone or in combination with Schmeidler.

Regarding the preceding paragraph, which was included in **both** the Response to the Final Action of March 31, 2008 **and** in the Amendment accompanying the Request for Continued Examination of June 16, 2008, the Examiner asserts in the current Office Action of August 6, 2008 that he disagrees "because the newly added prior art by Hart teaches quiesce time (see col. 16, lines 53-54)," merely repeating the same assertion made both in the Office Action of October 2, 2007 and the Final Action of March 31, 2008. **The Examiner has made no attempt to address the substance of Applicants' remarks.** The Examiner makes the further erroneous assertion that "Applicant did not define the phrase 'quiesce time' until this amendment." In fact, the amendment adding

"quiesce time" to claim 1 accompanied the Request for Continued Examination of July 26, 2007.

Further in regard to claim 1, contrary to the Examiner's assertion, the cited art does not teach or suggest the data access request is for data that is also accessible by one or more other clients each having a corresponding unexpired token, as recited in claim 1. The Examiner refers to Schmeidler, column 3, lines 47-51, as teaching this aspect of Applicants' claim. However, the cited portion of Schmeidler actually refers to security mechanisms to protect content from unauthorized access and replay. In particular, it discloses an authorization token from the conditional access server (CAS) indicating that the requesting user can have access to a specified briq (a portable, self-contained file system, containing all of the files necessary to run a particular title [column 2, lines 60-62]), on a specific RAFT file server, for the length of time spelled out in the negotiated payment type. There is no indication of a data access request for data that is **also accessible by other clients** ***each having a corresponding unexpired token***. Nor do any of the other cited references teach this aspect of Applicants' claim, whether considered alone or in combination with Schmeidler.

Further in regard to claim 1, contrary to the Examiner's assertion, the cited art does not teach or suggest wherein said quiesce time is a time when exclusive access to the data is required by a task, as recited in claim 1. The Examiner refers to Hart, column 16, lines 53-54, as teaching this aspect of Applicants' claim. However, the cited text refers to claim 3 of Hart, reciting "means to utilize said REBUILDINFO file to access said QUIESCE Time Stamp indicating the point in time to begin audit image application from audit disk (A1) to auxiliary data disk (D2)" Thus, the QUIESCE **time stamp** of Hart indicates when to begin an audit image application from an audit disk to an auxiliary data disk. Hart does not teach or suggest that quiesce time is a time when exclusive access to the data is required by a task, as recited in claim 1.

Further in regard to claim 1, the Examiner has not stated a proper reason to combine the teachings of the cited art, nor explained how to combine them. The

Examiner asserts that it would have been obvious to combine the teachings of Schmeidler with the teachings of Hart because "Hart's teachings would have allowed Schmeidler's method to provide a recovery method that can be measured in minutes (col. 2, lines 53-54)." However, Schmeidler is directed to encrypted, protected, secure delivery of purchased executable software content from a network file server to a client, whereas Hart is directed to **rapid recovery during failure of a primary active database by an auxiliary database**. The systems of Schmeidler and Hart are completely different types of systems. Schmeidler makes no mention of there being primary active and auxiliary databases, so that Hart's goal of recovery aimed at putting a multiple-node database in a physically consistent state is irrelevant. The quoted passage in Hart refers to recovering a multiple-node database into a physically consistent state "in minutes," and has no bearing on Schmeidler's system for encrypted, protected, secure delivery of purchased executable software content from a network file server to a client. Thus, one of ordinary skill would not have combined the teachings of Schmeidler with the teachings of Hart in the manner proposed by the Examiner. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness.

Further in regard to claim 1, contrary to the Examiner's assertion, the cited art does not teach or suggest generating an access token that grants the client access to data stored on one or more storage devices associated with the metadata server, **where the access token comprises an expiration time set by the metadata server to be no later than the maximum expiration time indicated by the next scheduled quiesce time**, as recited in claim 1. The Examiner again refers to Schmeidler, FIG.8, and to column 22, lines 65-66, as teaching this aspect of Applicants' claim. However, as already explained above, the token described in the cited portion of Schmeidler and illustrated in FIG. 8 as RAFT token 800, contains a start-time element 806 and an end-time element 808, which define the time interval during which the client may access a particular resource, namely the title the client has purchased. This has no bearing whatsoever on an expiration time set by the metadata server to be no later than **the maximum expiration time indicated by the next scheduled quiesce time**, which is a time at which *exclusive* access to certain

data is required by a task. Moreover, the token of Schmeidler is provided not by the network file server (RAFT server), but by the conditional access server (CAS).

In further regard to this aspect of claim 1, contrary to the Examiner's assertion, the cited art does not teach or suggest that the token expiration time is set *such that the access token will be expired during the next scheduled quiesce time, thus preventing the client from using the access token to access the data during the next scheduled quiesce time* as recited in claim 1. Admitting that Schmeidler and Hart do not teach this aspect of claim 1, the Examiner relies upon Ribot to remedy the deficiency. The Examiner refers to Ribot, paragraph [0036], as teaching this aspect of Applicants' claim. Ribot is directed to controlling access in client-server systems through a multi-level security protocol. At paragraphs [0035-0036], Ribot teaches that his invention accomplishes "the whole of the security and access controls during the authentication and authorization of the client organization. Thus, a set of objects containing the authorized privileges and credentials is distributed, and from this time on no further attention need be paid to it." This has absolutely no bearing upon *setting the expiration time of an **access token** to be no later than the maximum expiration time indicated by the next scheduled quiesce time such that the access token will be expired during the next scheduled quiesce time, thus preventing the client from using the access token to access the data during the next scheduled quiesce time*, as recited in claim 1. Ribot never discusses **expiration time**, much less **expiration time of access tokens**. Neither is there **any** discussion of **scheduled times of quiescence**, such as a scheduled freezing of the I/O to a specific file or dataset image in a shared storage environment. The cited portion of Ribot refers to the **time of authentication and authorization of the client** organization, when a set of objects containing the authorized privileges and credentials is distributed, from which time forward no further attention need be paid to it. This has nothing to do with a **scheduled time of quiescence**, or with setting an expiration time for an access token such that the access token will be expired during the next scheduled quiesce time, thus **preventing the client from using the access token to access the data during the next scheduled quiesce time**.

Further in regard to claim 1, the Examiner has not stated a proper reason to combine the teachings of the cited art, nor explained how to combine them. The Examiner asserts that it would have been obvious to combine the teachings of the cited references because Ribot's invention reduces the amount of unnecessary signaling in a **telecommunications** network, especially a **trunked radio telecommunications network which may be shared by two or more independent organizations** (page 2, paragraph [0011]). However, Schmeidler is directed to encrypted, protected, secure delivery of purchased executable software content from a network file server to a client. Not surprisingly, Schmeidler makes no reference whatsoever to a telecommunications network. Ribot, on the other hand, recites a network system of radio communications including a base transceiver station and a base network. The radio telecommunications services provided across the air interface between a base transceiver station and a user radio terminal are at least partly trunked [0029]. The Examiner cites Ribot's reducing unnecessary signaling in such a trunked radio telecommunications network as the reason that it would be **obvious** to combine Ribot with Schmeidler, whose invention is directed to encrypted, protected, secure delivery of purchased executable software content over the Internet. Aside from conjuring this startling justification for joining Ribot with Schmeidler, the Examiner leaves it entirely to the reader's imagination to create a link between this aspect of Ribot and the limitation of claim 1 for *setting the token expiration time such that the access token will be expired during the next scheduled quiesce time, thus preventing the client from using the access token to access the data during the next scheduled quiesce time*. Clearly one of ordinary skill would not have combined the teachings of Schmeidler with the teachings of Ribot as proposed by the Examiner. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness. Thus, one of ordinary skill would not have combined the teachings of the cited references in the manner proposed by the Examiner. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness.

Independent claims 6 and 11 recited limitations similar to those found in independent claim 1, and so the arguments presented above apply with equal force to the those claims, as well. For at least the above reasons, the cited references, whether

considered alone or in combination, clearly do not teach Applicants' independent claims 1, 6, and 11. Withdrawal of the rejections is respectfully requested.

In regard to claim 16, contrary to the Examiner's assertion, the cited art does not teach or suggest setting the expiration time of an access token to the earlier of either a maximum expiration time indicated by a next scheduled quiesce time or the default expiration time, wherein the access token grants a client access to data stored on one or more storage devices associated with a metadata server, and wherein the access token is set such that the access token will be expired during the next scheduled quiesce time, thus preventing the client from using the access token to access the data during the next scheduled quiesce time, as recited in claim 16. The Examiner refers to Schmeidler, FIG.8, and to column 22, lines 51-54 and lines 59-66, as teaching this aspect of Applicants' claim. However, the cited portion of Schmeidler actually refers to a token, illustrated in FIG. 8 as RAFT token 800, which contains a start-time element 806 and an end-time element 808, which define the **time interval** during which the client may access a particular resource, namely the title the client has purchased. There is absolutely no indication of setting the expiration time to ***the earlier* of either a *maximum expiration time indicated by a next scheduled quiesce time*, or *the default expiration time***. Nor do any of the other cited references teach this aspect of Applicants' claim, whether considered alone or in combination with Schmeidler.

Further in regard to claim 16, contrary to the Examiner's assertion, the cited art does not teach or suggest determining a default expiration time and setting the expiration time of an access token to the earlier of either a maximum expiration time indicated by a next scheduled quiesce time or the default expiration time, as recited in claim 16. The Examiner refers to McBrearty, paragraph [0004] as teaching this aspect of Applicants' claim. However, the cited portion of McBrearty only teaches that in a typical system, a security token has a limited lifetime, typically 24 hours before the token expires and the user must re-apply for a new token. Nowhere does McBrearty mention ***determining a default* expiration time**, or a **next scheduled quiesce time**, much less *comparing* the **determined default expiration time** and a **maximum expiration time indicated by a**

next scheduled quiesce time. Moreover, Schmeidler and Hart fail to overcome this deficiency of McBrearty.

Further in regard to claim 16, the Examiner asserts that it would have been obvious to combine the teachings of Schmeidler with the teachings of McBrearty because "McBrearty's teachings would have allowed Schmeidler's system and method for that (sic) allows for security tokens to be utilized which have more flexibility in a networked system (page 1, paragraph [0010])." The Examiner apparently intended to refer to paragraph [0009] of McBrearty, which refers to more flexible security tokens. However, even the proposed hypothetical combination of Schmeidler with McBrearty would not yield a system or method that includes the limitations of claim 16. At most it would allow Schmeidler to perform the sort of interruptions described in McBrearty at paragraph [0005]. But as McBrearty suggests at [0005], those interruptions would allow a system administrator to block access temporarily to prevent users from writing to the system, which would have no applicability in, and could even hamper, Schmeidler's system for securely *delivering on-demand content* over a broadband access network, where the client does not write to the system, but instead plays content such as audio, video, and animation which are stored on the network file server of Schmeidler. Thus, the references actually teach away from this combination, so that one of ordinary skill would not have combined the teachings of Schmeidler with the teachings of McBrearty in the manner proposed by the Examiner. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness.

Further in regard to claim 16, contrary to the Examiner's assertion, the cited art does not teach or suggest receiving a data I/O request associated with the access token, where the data I/O request is for data that is also accessible by one or more other clients each having a corresponding unexpired token, as recited in claim 16. The Examiner refers to Schmeidler, column 3, lines 47-51, as teaching this aspect of Applicants' claim. However, the cited portion of Schmeidler actually refers to security mechanisms to protect content from unauthorized access and replay. In particular, it discloses an authorization token from the conditional access server (CAS) indicating that the

requesting user can have access to a specified briq (a portable, self-contained file system, containing all of the files necessary to run a particular title [column 2, lines 60-62]), on a specific RAFT file server, for the length of time spelled out in the negotiated payment type. There is no indication that the data I/O request is for data that is **also accessible by one or more other clients** ***each having a corresponding unexpired token***.

Further in regard to claim 16, the Examiner notes that Schmeidler does not teach that the quiesce time is a time when exclusive access to the data is required by a task, as recited in claim 16. The Examiner refers to Hart, column 16, lines 53-54, as teaching this aspect of Applicants' claim. However, the cited text refers to claim 3 of Hart, reciting "means to utilize said REBUILDINFO file to access said QUIESCE Time Stamp indicating the point in time to begin audit image application from audit disk (A1) to auxiliary data disk (D2)" Thus, the QUIESCE **time stamp** of Hart indicates when to begin an audit image application from an audit disk to an auxiliary data disk. Hart does not teach that quiesce time is a time when exclusive access to the data is required by a task, as recited in claim 16.

Further in regard to claim 16, the Examiner asserts that it would have been obvious to combine the teachings of Hart with the teachings of McBrearty because "Hart's teachings would have allowed Schmeidler's method to provide a recovery method that can be measured in minutes (col.2, lines 53-54)." However, Schmeidler is directed to encrypted, protected, secure delivery of purchased executable software content from a network file server to a client, whereas Hart is directed to rapid **recovery during failure of a primary active database by an auxiliary database**. The systems of Schmeidler and Hart are completely different types of systems. Schmeidler makes no mention of there being primary active and auxiliary databases, so that Hart's goal of recovery aimed at putting a multiple-node database in a physically consistent state is irrelevant. The quoted passage in Hart refers to recovering a multiple-node database into a physically consistent state "in minutes," and has no bearing on Schmeidler's system for encrypted, protected, secure delivery of purchased executable software content from a network file server to a client. Thus, one of ordinary skill would not have combined the

teachings of Schmeidler with the teachings of Hart in the manner proposed by the Examiner. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness.

In further regard to claim 16, contrary to the Examiner's assertion, the cited art does not teach or suggest that the access token expiration time is set *such that the access token will be expired during the next scheduled quiesce time, thus preventing the client from using the access token to access the data during the next scheduled quiesce time*, as recited in claim 16. Admitting that Schmeidler and Hart and McBrearty to not teach this aspect of claim 16, the Examiner relies upon Ribot to remedy the deficiency. The Examiner refers to Ribot, paragraph [0036] as teaching this aspect of Applicants' claim. Ribot is directed to controlling access in client-server systems through a multi-level security protocol. At paragraphs [0035-0036], Ribot teaches that his invention accomplishes "the whole of the security and access controls during the authentication and authorization of the client organization. Thus, a set of objects containing the authorized privileges and credentials is distributed, and from this time on no further attention need be paid to it." This has absolutely no bearing upon *setting the access token* ***expiration time*** *such that the access token will be expired during the next scheduled quiesce time, thus preventing the client from using the access token to access the data during the next scheduled quiesce time*, as recited in claim 16. Ribot never discusses **expiration time**, much less **expiration time of access tokens**. Neither is there **any** discussion of **scheduled times of quiescence**, such as a scheduled freezing of the I/O to a specific file or dataset image in a shared storage environment. The cited portion of Ribot refers to the **time of authentication and authorization of the client** organization, when a set of objects containing the authorized privileges and credentials is distributed, from which time forward no further attention need be paid to it. This has nothing to do with a **scheduled time of quiescence**, or with setting an expiration time for an access token such that the access token will be expired during the next scheduled quiesce time, thus **preventing the client from using the access token to access the data during the next scheduled quiesce time**.

Further in regard to claim 16, the Examiner has not stated a proper reason to combine the teachings of the cited art, nor explained how to combine them. The Examiner asserts that it would have been obvious to combine the teachings of the cited references because Ribot's invention reduces the amount of unnecessary signaling in a **telecommunications** network, especially a **trunked radio telecommunications network which may be shared by two or more independent organizations** (page 2, paragraph [0011]). However, Schmeidler is directed to encrypted, protected, secure Internet delivery of purchased executable software content from a network file server to a client. Not surprisingly, Schmeidler makes no reference whatsoever to a telecommunications network. Ribot, on the other hand, recites a network system of radio communications including a base transceiver station and a base network. The radio telecommunications services provided across the air interface between a base transceiver station and a user radio terminal are at least partly trunked [0029]. The Examiner cites Ribot's reducing unnecessary signaling in such a trunked radio telecommunications network as the reason that it would be **obvious** to combine Ribot with Schmeidler, whose invention is directed to encrypted, protected, secure delivery of purchased executable software content over the Internet. Aside from conjuring this startling justification for joining Ribot with Schmeidler, the Examiner leaves it entirely to the reader's imagination to create a link between this aspect of Ribot and the limitation of claim 16 for *setting the access token expiration time such that the access token will be expired during the next scheduled quiesce time, thus preventing the client from using the access token to access the data during the next scheduled quiesce time*. Clearly one of ordinary skill would not have combined the teachings of Schmeidler with the teachings of Ribot as proposed by the Examiner. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness.

For at least the above reasons, the cited references, whether considered alone or in combination, clearly do not teach Applicants' independent claims 16. Withdrawal of the rejection is respectfully requested.

Applicants also assert that the rejection of numerous ones of the dependent claims is further unsupported by the cited art. However, since the rejections have been shown to be unsupported for the independent claims, a further discussion of the dependent claims is not necessary at this time.

Applicants note that the Examiner has made absolutely no attempt to address the *substance* of Applicants' previous arguments.

CONCLUSION

Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5760-19800/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicants

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: November 6, 2008